

Số: /KH-SNN

Tuyên Quang, ngày tháng 10 năm 2023

## KẾ HOẠCH

### Ứng phó sự cố đảm bảo an toàn thông tin mạng

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ đến năm 2020, định hướng đến năm 2025; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Thực hiện Kế hoạch số 197/KH-UBND ngày 19/10/2022 của Ủy ban nhân dân tỉnh về việc triển khai thực hiện Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng. Sở Nông nghiệp và Phát triển nông thôn ban hành kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng, như sau:

### I. MỤC ĐÍCH, YÊU CẦU

#### 1. Mục đích

- Đảm bảo an toàn thông tin cho các hệ thống thông tin quan trọng của Sở Nông nghiệp và PTNT; đảm bảo khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ đe dọa mất an toàn thông tin trên mạng; đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với lực lượng cán bộ, công chức, viên chức trong các cơ quan, đơn vị trực thuộc Sở.

- Bồi dưỡng, nâng lực, trình độ cho cán bộ phụ trách an toàn thông tin của Sở trong việc tiếp nhận, xử lý sự cố an toàn thông tin mạng, nâng cao kỹ năng xử lý thông tin đảm bảo linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố an toàn thông tin mạng.

#### 2. Yêu cầu

- Căn cứ trên kết quả khảo sát, đánh giá các nguy cơ, sự cố mất an toàn thông tin mạng của hệ thống thông tin của Sở để đưa ra phương án ứng phó, ứng cứu sự cố kịp thời, phù hợp.

- Các phương án ứng phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra.

- Xác định cụ thể các nguồn lực đảm bảo, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, đảm bảo khả thi, hiệu quả.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác đảm bảo an toàn thông tin giữa các cơ quan nhà nước trên địa bàn tỉnh; tăng cường sự phối hợp, hỗ trợ của Đội ứng cứu sự cố an toàn thông tin của tỉnh, Công an tỉnh và Sở Thông tin và Truyền thông tỉnh.

## **II. NỘI DUNG KẾ HOẠCH**

### **1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật về an toàn thông tin mạng**

Tổ chức tuyên truyền, phổ biến về Luật An toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 – 2020; Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP; Kế hoạch số 197/KH-UBND ngày 19/10/2022 của Ủy ban nhân dân tỉnh về việc triển khai thực hiện Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng; các văn bản chỉ đạo, triển khai của Sở về công tác đảm bảo an toàn thông tin mạng, Kế hoạch số 34/KH-SNN ngày 31/3/2022 về việc triển khai thực hiện Đề án “Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 - 2025”; Kế hoạch số 81/KH-SNN ngày 26/10/2023 về việc triển khai thực hiện Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030.

### **2. Tập huấn nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng cho cán bộ, công chức, viên chức**

Tập huấn nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng cho cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị; tham gia đầy đủ các khóa đào tạo, bồi dưỡng nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố do các Ủy ban nhân dân tỉnh và cơ quan chuyên môn tổ chức.

### **3. Xây dựng phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể.**

Việc xây dựng phương án đối phó, ứng cứu sự cố ATTT mạng phải đặt ra các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

a) Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp.

- Sự cố do bị tấn công mạng;
- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...;
- Sự cố do lỗi của người quản trị, vận hành hệ thống;
- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v...

b) Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống sau:

- Tình huống sự cố do bị tấn công mạng:
  - + Tấn công từ chối dịch vụ;
  - + Tấn công giả mạo;
  - + Tấn công sử dụng mã độc;
  - + Tấn công truy cập trái phép, chiếm quyền điều khiển;
  - + Tấn công thay đổi giao diện;
  - + Tấn công mã hóa phần mềm, dữ liệu, thiết bị;
  - + Tấn công phá hoại thông tin, dữ liệu, phần mềm;
  - + Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;
  - + Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;
  - + Các hình thức tấn công mạng khác.
- Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:
  - + Sự cố nguồn điện;
  - + Sự cố đường kết nối Internet;
  - + Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;
  - + Sự cố liên quan đến quá tải hệ thống;
  - + Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.
- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống:

- + Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;
  - + Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;
  - + Lỗi liên quan đến chính sách và thủ tục an toàn thông tin;
  - + Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;
  - + Lỗi khác liên quan đến người quản trị, vận hành hệ thống.
- Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v....

c) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, giữa các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố;

d) Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ, và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể.

#### **4. Triển khai phòng ngừa sự cố; giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố**

- *Các nội dung, nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm:*
  - + Thực hiện nghiêm công tác giám sát, phát hiện sớm nguy cơ, sụp đổ;
  - + Kiểm tra, đánh giá ATTT mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc;
  - + Phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro an toàn thông tin mạng, phần mềm độc hại;
  - + Xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.
- *Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố:*
  - + Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ ứng cứu, khắc phục sự cố hoặc thuê dịch vụ bảo đảm an toàn thông tin;
  - + Chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; thuê dịch vụ kỹ thuật, đơn vị chuyên gia tư vấn, hỗ trợ ứng cứu sự cố.

### **III. TỔ CHỨC THỰC HIỆN**

#### **1. Các phòng chuyên môn, đơn vị trực thuộc Sở**

- Căn cứ chức năng nhiệm vụ được giao tại Kế hoạch này có trách nhiệm tổ chức, triển khai thực hiện tại cơ quan, đơn vị. Quan tâm, chú trọng đến công tác bảo đảm an toàn thông tin mạng cho hệ thống thông tin; chủ động bố trí kinh phí trang bị phần mềm chống virus cho hệ thống mạng, hệ thống thông tin của đơn vị.

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an toàn thông tin mạng; có trách nhiệm cử cán bộ, công chức phối hợp với bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng của Sở trong công tác ứng phó, xử lý các sự cố an toàn thông tin của đơn vị, của Sở.

## **2. Giao Văn phòng Sở**

- Làm đầu mối tiếp nhận sự cố an toàn thông tin của Sở, có trách nhiệm theo dõi, đôn đốc, đánh giá và hướng dẫn các phòng chuyên môn, các đơn vị trực thuộc Sở trong quá trình triển khai thực hiện.

- Chủ trì, phối hợp với các phòng, đơn vị trực thuộc Sở xây dựng xây quy trình xử lý đối phó, ứng cứu đối với một số tình huống sự cố cụ thể được nêu tại Mục 3 Phần II của kế hoạch này. Định kỳ hàng năm hoặc theo hướng dẫn của cơ quan chuyên môn tiến hành kiểm tra các công tác bảo đảm ATTT tại cơ quan, đơn vị.

- Tham mưu đưa nội dung dự phòng kinh phí, nhân lực thường trực sẵn sàng ứng cứu sự cố; triển khai điều hành phối hợp tổ chức ứng cứu và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố vào các kế hoạch về bảo đảm ATTT mạng, ứng dụng công nghệ thông tin.

- Trường hợp sự cố ngoài phạm vi khả năng hỗ trợ phải báo cáo Lãnh đạo Sở xin hỗ trợ từ các cơ quan chuyên trách ứng cứu sự cố của tỉnh hoặc liên hệ đầu mối thông báo sự cố Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616, Email: ais@mic.gov.vn.

Trên đây là kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng tại Sở Nông nghiệp và PTNT. Yêu cầu các đơn vị nghiêm túc triển khai thực hiện./.

### ***Nơi nhận:***

- Sở Thông tin và Truyền thông;
- Lãnh đạo Sở;
- Các phòng, đơn vị trực thuộc Sở;
- Trang TTĐT;
- Lưu: VT, VP.

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**Nguyễn Công Hàm**